RSAC 2025 Conference

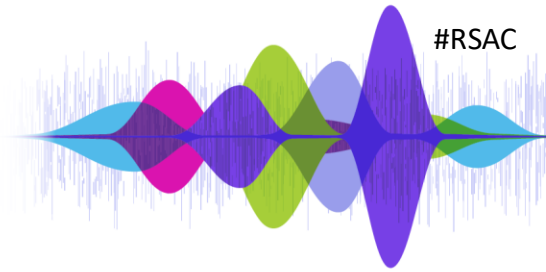
Many Voices.
One Community.

SESSION ID: LAB1-M01

Resilient by Design: Lessons from the CrowdStrike Incident

Matthew Chiodi

Chief Trust Officer
Cerby
https://rb.gy/zpabw7

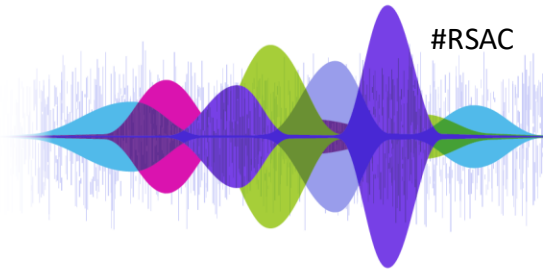


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



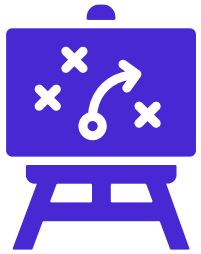
What is cyber resilience?

"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."
(NIST SP 800-160)

PLAIN ENGLISH

The ability to prepare for, keep running during, and bounce back from cyberattacks or other problems that affect technology and systems.

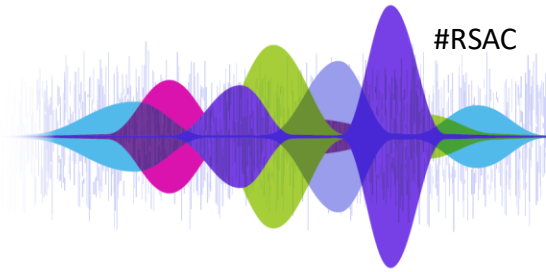
Three key elements



ANTICIPATE
PREPARE FOR POTENTIAL CYBER THREATS BEFORE THEY OCCUR

WITHSTAND
MAINTAIN OPERATIONS DURING CYBER INCIDENTS

RECOVER AND ADAPT
RESTORE AND IMPROVE OPERATIONS POST-INCIDENT



CrowdStrike is a cybersecurity company that provides cloud-delivered protection of endpoints, cloud workloads, identity, and data.

CROWDSTRIKE

STATS

Revenue: $3B in 2024

Employees: 7,925

Market cap: $110B

Customers: 23k

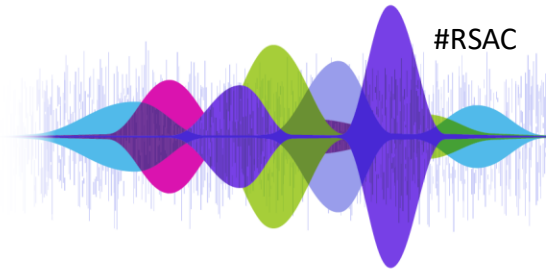
What does the Falcon Sensor do?

- **REAL-TIME PROTECTION:**
  RUNS AT THE KERNEL LEVEL TO DETECT AND BLOCK ADVANCED THREATS LIKE MALWARE AND RANSOMWARE.

- **AI-DRIVEN DETECTION:**
  LEVERAGES AI AND MACHINE LEARNING WITH CLOUD-BASED ANALYSIS FOR CONTINUOUS, ADAPTIVE SECURITY.

- **LIGHTWEIGHT & CLOUD-MANAGED:**
  MINIMAL IMPACT ON DEVICE PERFORMANCE (<30 MB) WITH NO NEED FOR LOCAL UPDATES, ALL MANAGED VIA THE FALCON CLOUD.

The timeline



FEBRUARY 2024

Initial Falcon sensor capability released.

MARCH 2024

First successful Channel File 291 update.

APRIL 2024

Three additional successful updates.

12:09 AM ET, JULY 19, 2024

Faulty Falcon update released, leading to global crashes.

1:27 AM ET, JULY 19, 2024

Fix issued **(78 minutes after discovery).**

JULY 25, 2024

Additional runtime checks added to the driver.

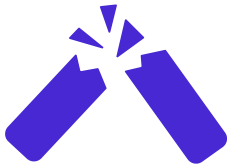
AUGUST 9, 2024

Full patch applied globally.

Global impact

TOTAL LOSSES

F500 ~$5.4B



DISRUPTIONS

Airlines - 7k flights cancelled

Healthcare - ER wait times 4+ hours

Finance - 10M failed transactions

Retail - 25% drop in e-commerce

Transportation - delayed 300k shipments

INSURANCE GAP

80-90% not covered

Lessons learned

- **PREPARATION IS CRITICAL**

  Incident response and business continuity plans allow for fast, effective mitigation.

- **TEST YOUR PLANS**

  Regular practice of incident response protocols ensures quicker recovery.

- **CLEAR COMMUNICATION**

  Timely, consistent updates to staff and stakeholders help maintain calm and control.

- **DIG DEEP INTO YOUR VENDOR'S DR PLANS**

  Ask questions and inspect.

- **CHECK YOUR INSURANCE COVERAGE**

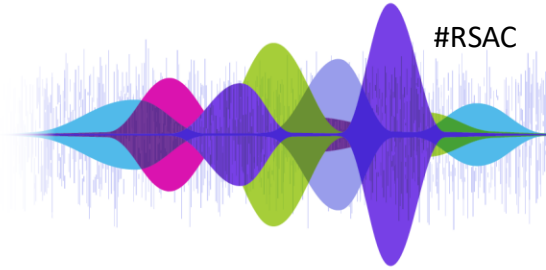
  Don't just check the box. Work with your carrier to ensure adequate coverage.

RSAC 2025 Conference

Questions?

Get ready to collaborate!

Applying NIST CSF to the CrowdStrike Incident



- **Objective:** Analyze the **CrowdStrike Incident** using the **NIST Cybersecurity Framework (CSF)** to uncover failures and resilience strategies.

- **Format:**

  Each table is assigned **one of the five NIST CSF functions** (Identify, Protect, Detect, Respond, Recover).

- **Discuss your function** in the context of the CrowdStrike failure.

- **Answer the key questions on your handout** and prepare **one key takeaway to share.**

Timing:

✅ **5 mins:** Table assignments & scenario introduction
✅ **20 mins:** Group discussions
✅ **10 mins:** Rapid share-out

cerby

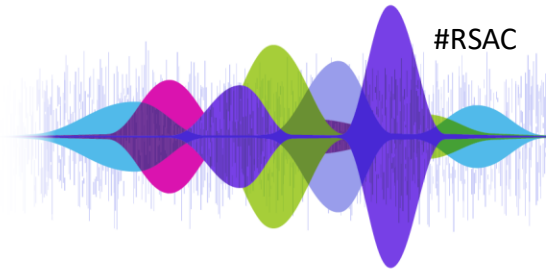
Team roles and how to run your table

- Each table should assign the following roles to ensure an effective discussion:
  - 👤 **Facilitator** – Keeps the conversation focused and ensures all voices are heard.
  - 📝 **Note-Taker** – Captures key insights and recommendations.
  - 📣 **Spokesperson** – Presents the table's findings during the group share-out.

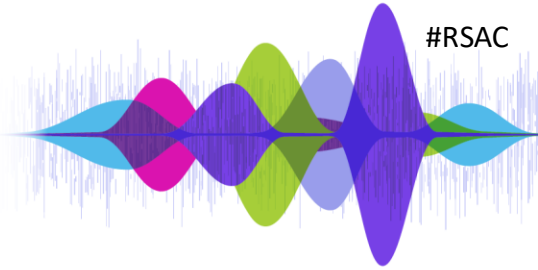
Running Your Discussion (20 Minutes)

- **Step 1 (5 mins):** Read your assigned **NIST CSF function** and the key questions.
- **Step 2 (10 mins):** Discuss the **CrowdStrike failure** through your function's lens.
- **Step 3 (5 mins):** Summarize **one key insight** and **one recommendation** for the share-out.

Timer on-screen slide



Group share-out (2 minutes by function)



✅ **State your NIST CSF function (Identify, Protect, Detect, Respond, Recover).**

✅ **Share ONE key insight** your table discussed.

✅ **Provide ONE recommendation** for improving resilience based on this incident.

- **Discussion Prompts (After Share-Out)**
  - *What patterns emerged across the five CSF functions?*
  - *What resilience gaps did enterprises overlook?*
  - *What's one immediate action security leaders should take based on this session?*

RSAC 2025 Conference

Preparing for the unknown, unknowns

Cyber Resilience Review (CRR)

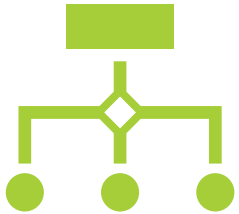
Many Voices.
One Community.

Understanding the CRR

- Developed by CISA to assess an organization's cyber and operational resilience.
- Non-technical, risk-based approach focused on business continuity & security.
- Helps organizations identify gaps before disruptions occur.

Why the CRR matters

Beyond Security
Focuses on business continuity, third-party risk, and recovery.



Actionable
Aligns with NIST CSF, ISO 27001, and CIS Controls.

Proactive
Identifies gaps in response & resilience before incidents happen.

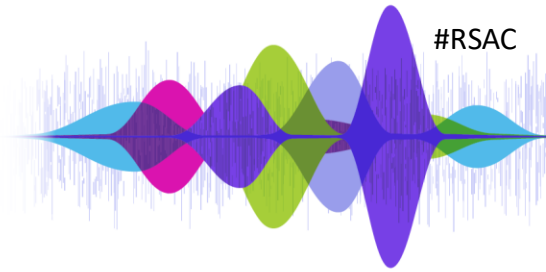
CRR's 10 key domains

- Asset Management
- Controls Management
- Configuration & Change Management
- Vulnerability Management
- Incident Management
- Service Continuity Management
- Risk Management
- External Dependency Management
- Training & Awareness
- Situational Awareness

Get ready to collaborate!

Table assignments and roles

Table	Department (CRR Domain)	Your responsibility
1-2	IT Operations (Asset Management)	Identify which critical assets depend on the SaaS vendor & assess potential workarounds.
3-4	Vendor Management (External Dependency Management)	Contact the SaaS vendor, demand transparency, and determine if contractual obligations cover this scenario.
5-6	SOC / Incident Response (Incident Management)	Investigate the attack, determine scope of exposure, and coordinate containment.
7-8	Business Continuity (Service Continuity Management)	Develop immediate contingency plans—can we switch vendors or activate backups?
9-10	CISO / Risk Office (Risk Management)	Assess legal, compliance, and financial risks of different response options (e.g., waiting, switching vendors, communicating publicly).
11	HR & Awareness Team (Training & Awareness)	Manage internal employee communications—how do we prevent panic and keep business running?
12	Threat Intelligence Team (Situational Awareness)	Analyze external threats—was this attack part of a broader campaign? What are other companies doing?
13	🚨 The Vendor (Crisis Decision-Makers)	Respond to customer demands, make key ransomware decisions (pay or not?), and determine recovery timeline.



Scenario briefing

Your company relies on a major SaaS CRM provider. This morning at 9:00 AM, employees report they can't log in. By 10:30 AM, the vendor confirms a "service disruption." No further details have been shared. Customers are noticing issues, and executives are asking for answers.

💡 First Decisions (3 Minutes):

- What critical business functions depend on this SaaS provider?
- Who on your team needs to be pulled in to assess the risk?
- What's your next step—wait for vendor updates or take action?

Discuss & interact—tables/teams must check in with at least two others.

Breaking news pt. 1

The SaaS vendor has confirmed they are experiencing a ransomware attack. All operations have been shut down. No estimated time for recovery. Customers are now complaining on social media.

New Decisions (5 Minutes):

- **Do you inform your customers or wait for more details?**
- **What alternative solutions do you have in place?**
- **How do you communicate this internally—do you escalate to the board?**

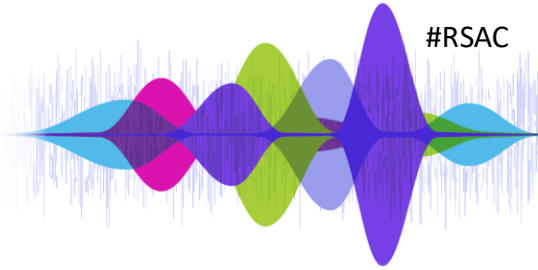
Breaking news pt. 2

📢 *The vendor has received a ransom demand of $15 million. They are considering whether to pay. Your executive team wants to know: What happens if they don't recover in the next 48 hours?*

💡 **New Decisions (5 Minutes):**

- Do you pressure the vendor to disclose their response plan?
- Should your company develop a contingency plan to replace this service?
- What's your legal and compliance risk if the data is exposed?

Breaking news pt. 3



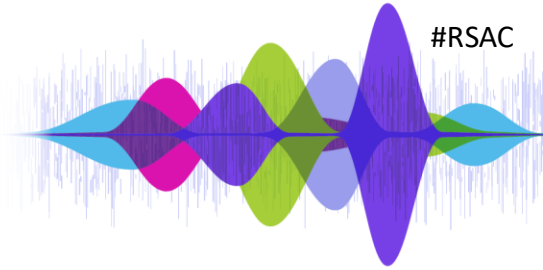
A journalist reaches out for a statement: 'We have sources confirming that your company's operations are impacted by a ransomware attack on Vendor X. Would you like to comment?' Your leadership needs an answer NOW.

💡 **Final Decisions (5 Minutes):**

- **How do you handle public communication?**
- **What's your long-term resilience improvement to avoid this again?**
- **How do you ensure your vendors have proper security controls?**

✅ **Give teams 5 minutes to finalize their decisions before share-outs.**

Table share-out



- **Five tables present** their boldest decision (90 seconds each).
- Facilitator **highlights patterns** across different teams.
- **Key Reflection:** *What would your real company do differently after this exercise?*

Applying Cyber Resilience in Your Organization (Next Week)

🚀 **Immediate Actions to Take in the Next Week:**

✅ **Assess Vendor Dependencies:** Identify all critical third-party services your business relies on.

✅ **Review Incident Response Plans:** Ensure your organization has a clear process for vendor-related disruptions.

✅ **Talk to Key Stakeholders:** Start a conversation with IT, Security, and Business Continuity teams about resilience gaps.

💡 *Key Question: If a key vendor suffered a major outage today, how prepared would your organization be?*

Strengthening Resilience Over the Next Three Months

📌 **Actions to Implement in 90 Days:**

🔹 **Map Business-Critical Vendors** – Identify primary and backup SaaS/service providers.

🔹 **Evaluate Third-Party Risk Policies** – Do your contracts include security and resilience expectations?

🔹 **Run a Tabletop Exercise** – Simulate a vendor outage and test your response plan.

🔹 **Engage Leadership** – Educate executives on the **business impact** of vendor failures.

🔹 **Assess Incident Communication Plans** – Ensure clear messaging for customers, regulators, and employees.

💡 *Key Question: Do you have contractual leverage to demand transparency and rapid remediation from vendors?*

Long-Term Cyber Resilience Investments (6+ Months Out)

🏆 **Building Sustainable Resilience:**

📍 **Define a Vendor Risk Triage System** – Establish internal criteria for evaluating vendor resilience.

📍 **Automate Vendor Risk Monitoring** – Use technology to track real-time security signals from suppliers.

📍 **Expand Backup & Redundancy Strategies** – Can critical services fail over seamlessly?

📍 **Strengthen Security Requirements in Contracts** – Ensure vendors provide transparency & response commitments.

📍 **Develop a Cross-Team Resilience Culture** – Embed resilience into procurement, legal, and IT processes.

💡 *Key Question: How will your organization measure and track vendor resilience over time?*

cerby

RSAC™ | 2025 Conference

Many Voices.
One Community.